
Index

- $3n + 1$ problem, 51

- AARONSON, Scott, 73
- absolute value, 9
- ACKERMANN, Wilhelm
 - Ackermann function, 68
- ADLEMAN, Leonard, 1, 132, 135, 192
- age of the universe, 40
- AGRAWAL, Manindra, 163
- AKS algorithm, 4, 186
- AL-KHWARIZMI, Abu Abdallah
 - Muhammad ibn Musa, 50
- ALBERTI, Leon Battista, 131
- algorithm, 43, 45
 - ADDITION, 46, 61
 - AKS, 4, 186
 - COLLATZ, 51
 - CRIME-BESTSELLER, 44
 - deterministic, 73
 - efficient, 60
 - Euclidean, 29, 35, 36, 43, 50, 66
 - inefficient, 40
 - Karatsuba, 67
 - Las Vegas, 77
 - MILLER-RABIN, 145
 - Monte Carlo, 75
 - $N^*(PI+E)$, 48
 - of Agrawal, Kayal, and Saxena, 4, 186
 - PANCAKE, 44
 - QUICKSORT, 76
 - randomized, 73
 - Schönhage-Strassen, 68
 - analysis
 - mathematical, 143
 - Annals of Mathematics*, 4, 25, 199
 - ARENSTORF, Richard F., 204
 - arithmetic
 - modular, 84
 - arithmetic progression, 199
 - asymptotic growth, 59
 - asymptotic running time, 60
 - average running time, 78
 - axiom, 14
 - Peano axioms, 25

- BACHMANN, Paul, 66
 - base, 104
 - basis of the induction, 17
 - best-selling crime novel, 44
- BÉZOUT, Étienne
 - Bézout's Lemma, 37, 39, 87
- binary number system, 46, 51
- binomial coefficients, 19
 - explicit formula, 23
 - recursive formula, 19
- binomial theorem, 19
- BISWAS, Somenath, 163
- bounded from above/below, 22

- CAESAR, Julius, 66
 - Caesar cipher, 130
- calculus
 - integral/differential, 143
- CARMICHAEL, Robert D.
 - Carmichael number, 106, 107, 146
- CHEBYSHEV, Pafnuty Lvovich, 139
- CHEN, Jingrun, 195, 198
- Chinese Remainder Theorem, 89
- CHURCH, Alonzo, 50, 54
- Church-Turing thesis, 50
- cipher
 - digraphic substitution, 131
 - mono-alphabetic, 130
 - playfair, 131
 - poly-alphabetic, 131
 - RSA, 132
- ciphertext, 130
- Clement's Theorem, 199
- CLEMENT, Paul A.
 - Clement's Theorem, 199
- coefficient, 108
 - leading, 108
- Collatz Conjecture, 51
- COLLATZ, Lothar, 51
- colorability, 70
- combinatorics, 19
- common divisor, 27
 - greatest, 27
- common factor, 27
 - highest, 27
- common multiple, 27
 - least, 27
- complete set of residues, 92
- complex numbers, 181, 193, 203
 - complex analysis, 139
- complexity theory, 58
- composite number, 26
- COMPOSITES, 53
- conclusion, 6
- congruence, 84
 - modulo a polynomial, 113
 - of polynomials modulo n , 120
- congruence class, 93
- congruent, 84
- constant polynomial, 108
- contradiction
 - proof by, 15
- converse, 7
- coprime, 27
- corollary, 7
- coset, 100
- counterexample
 - smallest, 15
- cryptology, 129
 - public-key, 132
- CSR, 92
- cyclotomic polynomial, 178

- DE LA VALLÉE POUSSIN, Charles-Jean, 139
- DE VIGENÈRE, Blaise, 131
- decidable problem, 52
- decimal number system, 51
- decision problem, 52
- decomposition
 - into irreducible factors, 125
 - into prime factors, 31
- defined as, 8
- definition, 6
 - recursive, 18
- degree of a polynomial, 108
 - modulo n , 121
- descent
 - infinite, 15
- determinism, 45
- deterministic algorithm, 73
- diagonalization, 57
- differential calculus, 143
- DIFFIE, Whitfield, 135
- digraphic substitution ciphers, 131
- Diophantine equation, 92
- direct proof, 18
- DIRICHLET, Gustav Lejeune
 - Dirichlet's Prime Number Theorem, 200
 - Disquisitiones Arithmetica*, 34
- divide and conquer, 62
- division
 - long, 29
 - polynomial long division, 110
 - with remainder, 28
- division algorithm, 28
- division theorem, 28
- division with remainder, 28

- for polynomials, 111
- divisor, 26
 - common, 27
 - greatest common, 27
 - non-trivial, 26
 - of a polynomial, 110, 112
 - of a polynomial modulo n , 122
 - trivial, 26
 - zero, 119
 - zero divisor, 91, 93
- dual problem, 53
- efficiency, 60
- efficiently verifiable problem, 69
- EISENSTEIN, Ferdinand, 203
 - irreducibility criterion, 126
- elements of a set, 8
- empty set, 8
- encryption
 - RSA, 2
- Entscheidungsproblem, 50, 54
- ERATOSTHENES of Cyrene, 40
 - Sieve of, 39, 43, 61
- EUCLID, 34, 38, 41, 200
- Euclid number, 200
- Euclidean algorithm, 29, 35, 36, 43, 50, 66
- EULER, Leonhard, 194, 195
 - Euler's constant, 9
 - Fermat-Euler Theorem, 99
 - phi function, 104
 - totient function, 98, 104
- even integers, 7
- even number, 22, 84
- factorial, 9
- Factoring Challenge, 2
- Fermat number, 203
- Fermat prime, 203
- Fermat test, 105
- FERMAT, Pierre de, 2, 25
 - Fermat's Last Theorem, xi, 25, 189, 191
 - Fermat's Little Theorem, 25, 96
 - Fermat-Euler Theorem, 99
 - Last Theorem of, 197
 - theorem of Fermat-Miller, 145
- Fibonacci numbers, 19, 66
- field, 93
- finite arithmetic progression, 199
- FOUVRY, Étienne, 190, 191
- fraction, 7
- frequency analysis, 130
- function, 9
 - one-way, 132
- Fundamental Theorem of Arithmetic, 31
- FÜRER, Martin, 68
- GAUSS, Carl Friedrich, 104, 139
 - Disquisitiones Arithmetica*, 34
 - Gauss summation, 22
- gcd, 27
- Generalized Riemann Hypothesis, 149, 192, 195
- GERMAIN, Sophie, 189, 191, 202
- GÖDEL, Kurt, 57
 - incompleteness theorem, 57
- GOLDBACH, Christian, 195
 - Goldbach Conjecture, 195
 - Weak Goldbach Conjecture, 196
- Goldberg's Conjecture, 197
- graph, 56
- Great Internet Mersenne Prime Search, 201
- greatest common divisor, 27
- GREEN, Ben
 - Green-Tao Theorem, 199
- group, 104
- HADAMARD, Jacques, 139
- halting problem, 54
- HARDY, Godfrey Harold, 1, 190, 205
- HEATH-BROWN, David Rodney, 192
- HELFGOTT, Harald, 197
- HELLMAN, Martin, 135
- highest common factor, 27
- Hilbert's decision problem, 54
- HILBERT, David, 49, 194
 - Entscheidungsproblem, 50, 54
 - Tenth Problem, 56
- hypothesis, 6
- induction
 - basis of, 17
 - mathematical, 16

- variants, 18, 25
- induction hypothesis, 17
- induction step, 17
- inefficient algorithm, 40
- infinite descent, 15
- input, 52
- instance, 52
 - positive/negative, 53
- integer, 7
 - even, 7
 - odd, 7
- integral, 143
- integral calculus, 143
- integral domain, 119
- integral logarithm, 139
- intractable problem, 60
- inverse modulo n , 87
- irreducible polynomial, 114
 - Eisenstein criterion, 126
 - modulo p , 123
- Jacobi symbol, 149
- KARATSUBA, Anatoly Alexeevitch
 - Karatsuba algorithm, 67
- KASISKI, Friedrich W., 131
- key
 - private, 132
 - public, 132
- LAGRANGE, Joseph-Louis
 - Lagrange's Theorem, 101, 104
- LANDAU, Edmund
 - Landau symbols, 66
- Las Vegas algorithm, 77
- Las Vegas method, 73
- lcm, 27
- leading coefficient, 108
- least common multiple, 27
- Legendre symbol, 149
- LEGENDRE, Adrien-Marie, 139
- lemma, 7
 - Bézout's Lemma, 39, 87
- LENSTRA, Hendrik W., 190
- Library of Alexandria, 40
- linear factor, 112, 117, 124
- LITTLEWOOD, John E., 190, 205
- logarithm
 - base 2, 9
 - integral, 139
 - natural, 9
- Logarithmic Integral Function, 193
- long division, 29
 - polynomial, 110
- LUCAS, Édouard
 - Lucas test, 201
- MARKOV, Andrei Andreyevich
 - Markov inequality, 78, 81
- mathematical analysis, 143
- mathematical induction, 16
 - variants, 18, 25
- Mersenne prime
 - Great Internet Mersenne Prime Search, 201
- MERSENNE, Marin
 - Mersenne number, 200
 - Mersenne prime, 201
- Millennium Prize Problems, 72, 194
- MILLER, Gary Lee, 3, 149
 - theorem of Fermat-Miller, 145
- Miller-Rabin primality test, 145
- modular arithmetic, 84
 - modulo a polynomial, 113
- monic, 108
- mono-alphabetic cipher, 130
- Monte Carlo algorithm, 75
- Monte Carlo method, 73
- multiple, 17, 26
 - common, 27
 - least common, 27
- multiplicative inverse, 87
- National Lottery, 19
- natural logarithm, 9
- natural numbers, 7, 13
- negative instance, 53
- non-trivial divisor, 26
 - of a polynomial, 112
- NP, 68, 69
- NP-complete problem, 72
- number
 - Carmichael, 106, 107
 - complex, 181, 193, 203
 - composite, 26
 - Euclid, 200
 - even/odd, 22, 84

- integer, 7
- natural, 7, 13
- perfect, 200
- prime, 1, 26
- rational, 7
- real, 7
- number of atoms in the universe, 40, 68, 197
- O*-notation, 59, 66
- odd integers, 7
- odd number, 22, 84
- one-way function, 132
- order modulo n , 94
- output, 52
- P**, 60
- pairwise, 23
- pancake, 44
- particle physics, xi
- Pascal's triangle, 19, 96
- PAUSANIAS, 130
- Peano axioms, 25
- PEANO, GIUSEPPE, 25
 - Peano axioms, 25
- perfect number, 200
- perfect power, 9
- plaintext, 130
- playfair cipher, 131
- poly-alphabetic cipher, 131
- Polybius square, 130
- polynomial, 108
 - constant, 108
 - cyclotomic, 178
 - in $X/Y/Z$, 109
 - in several variables, 56, 73
 - integer/rational, 108
 - irreducible, 114
 - irreducible (modulo p), 123
 - monic, 108
 - over a field, 119
 - reducible, 118
 - zero, 108
- polynomial running time, 60
- polynomial zero, 116, 123
- POMERANCE, Carl, 190
- positive instance, 53
- POST, Emil
 - Correspondence Problem, 56
- power
 - perfect, 9
- PRATT, Vaughan, 72
- prime, 1, 26
 - Fermat, 203
 - Mersenne, 201
 - root of unity modulo a prime, 144
 - Sophie Germain prime, 190
 - twin, 42
- prime factor, 30
- prime factor decomposition, 31
- prime gap, 41
- prime number theorem, 137
- PRIMES, 53
- primitive root, 103
- primitive root of unity, 181
- private key, 132
- problem, 52
 - $3n + 1$, 51
 - class **NP**, 68, 69
 - class **P**, 60
 - class **RP**, 75
 - class **ZPP**, 78
 - COMPOSITES, 53
 - decision, 52
 - dual, 53
 - efficiently computable, 60
 - efficiently verifiable, 69
 - halting problem, 54
 - Hilbert's Entscheidungsproblem, 50, 54
 - Hilbert's Tenth Problem, 56
 - intractable, 60
 - NP**-complete, 72
 - Post Correspondence Problem, 56
 - PRIMES, 53
 - search, 52
 - SUM, 52
 - (un)decidable, 52
- product notation, 8
- proof, 6
 - by contradiction, 15
 - direct, 18
- pseudo-prime, 105
- strong, 146

- public key, 132
- public-key cryptography, 132
- Quicksort, 76
- RABIN, Michael Oser, 3, 149
- RAMARÉ, Olivier, 196
- randomized algorithm, 73
- rational numbers, 7
- real numbers, 7
- recursive definition, 18
- reduced set of residues, 92
- reducible polynomial, 118
- Riemann ζ -function, 193
- Riemann Hypothesis, 139, 193
 - Generalized, 149, 192, 195, 197
- RIEMANN, Bernhard, 193
- RIVEST, Ronald, 1, 132, 135
- root of unity, 181
 - modulo a prime, 144
 - primitive, 181
- RP**, 75
- RSA, 2, 132
- RSA number, 2
- RSR, 92
- running time
 - asymptotic, 60
 - average, 78
 - exponential, 60
 - function, 58
 - polynomial, 60
- SCHÖNHAGE, Arnold, 68
- Schönhage-Strassen algorithm, 68
- search problem, 52
- set, 8
 - uncountable, 57
- SHAMIR, Adi, 1, 132, 135
- Sieve of Eratosthenes, 39, 43, 61
- Skytale, 130
- smallest counterexample, 15
- SOLOVAY, Robert Martin, 149
- Sophie Germain prime, 190, 202
- STRASSEN, Volker, 68, 149
- string, 52, 58
- strong pseudo-prime, 146
- subset, 8
- successor, 24
- sufficiently large, 59
- sum notation, 8
- SYLVESTER, James Joseph, 104
- TAO, Terence, 199
 - Green-Tao Theorem, 199
- TENENBAUM, Gérald, 204
- theorem, 7
- theorem of Agrawal, Kayal, and Saxena, 169
- theorem of Fermat-Miller, 145
- totient function, 98
- triples of prime numbers, 198
- trivial divisor, 26
- TURING, Alan, 50, 54, 131
- twin primes, 42, 197
- uncountable set, 57
- undecidable problem, 52
- unique modulo n , 88
- universe
 - age, 40
 - number of atoms, 40, 68, 197
- Vigenère square, 131
- VINOGRADOV, Ivan Matveyevich
 - Vinogradov's Theorem, 196
- VON KOCH, Helge, 139, 194
- Weak Goldbach Conjecture, 196
- well-ordering principle, 14
- What's my line?, 62
- WHEATSTONE, Charles, 131
- WILES, Andrew, xi, 25, 192
- Wilson's Theorem, 149, 204
- WILSON, John, 149, 204
- witness, 69
- zero
 - polynomial, 116, 123
- zero divisor, 91, 93, 115, 119
- zero of a polynomial, 109
- zero polynomial, 108
- ZHANG, Yitang, 198
- ZPP**, 78